Bank _____ **Date of Exam** _____
Charter _____ **Prepared By** _____

#14 - IDENTITY THEFT RED FLAGS

OVERVIEW

The identity theft red flags rule requires a financial institution to periodically determine whether it offers or maintains accounts covered by the regulation. A covered account generally is a consumer account or any other account the institution determines carries a foreseeable risk of identity theft. For covered accounts, an institution must develop and implement a written identity theft prevention program (program) that is designed to detect, prevent, and mitigate identity theft in connection with any new or existing covered account. The program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities. Financial institutions may draw upon their existing programs, such as Bank Secrecy Act/Anti-Money Laundering compliance programs, customer identification programs, or customer information security programs, to help formulate their identity theft prevention program.

CORE ANALYSIS

Detection, Prevention, and Mitigation of Identity Theft

After an initial evaluation, subsequent examinations should be risk-focused in scoping future reviews.

1. Determine if the bank periodically identifies covered accounts it offers or maintains. Verify that the bank:

- Included accounts for personal, family, and household purposes that permit multiple payments or transactions; and
- Conducted a risk assessment to identify any other accounts that pose a reasonably foreseeable risk of identity theft, taking into consideration the methods used to open and access accounts, and the institution's previous experiences with identity theft (12 CFR 222.90(c)).

Refer to **Appendix** for information on Identity Theft Red Flags and 12 CFR 222 Subpart J.

Comment:

2. Review examination findings in other areas (e.g. Bank Secrecy Act, Customer Identification Program and Customer Information Security Program) to determine whether there are deficiencies that adversely affect the financial institution's ability to comply with the Identity Theft Red Flags Rules (red flag rules).

Comment:

3. Review any reports, such as audit reports and annual reports prepared by staff for the board of directors (or an appropriate committee thereof or a designated senior management employee) on compliance with the red flag rules, including reports that address:

- The effectiveness of the financial institution's Identity Theft Prevention Program (Program);
- Significant incidents of identity theft and management's response;
- Oversight of service providers that perform activities related to covered accounts; and
- Recommendations for material changes to the Program.

Determine whether management adequately addressed any deficiencies (12 CFR 222.90(f); Guidelines, Section VI).

Comment:

4. Verify that the financial institution has developed and implemented a comprehensive written Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account. The Program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities (12 CFR 222.90(d)(1)).

- Verify that the financial institution considered the Guidelines in **Appendix J** to the regulation (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation) in the formulation of its Program and included those that are appropriate (12 CFR 222.90(f)).
- Determine whether the Program has reasonable policies, procedures, and controls to effectively identify and detect relevant red flags and to respond appropriately to prevent and mitigate identity theft (12 CFR 222.90(d)(2)(i)-(iii)). Financial institutions may, but are not required to, use the illustrative examples of red flags in **Supplement A** to the Guidelines to identify relevant red flags (12 CFR 222.90(d)(2); Appendix J, Sections II, III and IV).
- Determine whether the financial institution uses technology to detect red flags. If it does, discuss with management the methods by which the financial institution confirms the technology is working effectively.
- Determine whether the Program (including the red flags determined to be relevant) is updated periodically to reflect changes in the risks to customers and the safety and soundness of the financial institution from identity theft (12 CFR 222.90(d)(2)(iv)).
- Verify that (i) the board of directors (or appropriate committee thereof) initially approved the Program; and (ii) the board (or an appropriate committee thereof, or a designated senior management employee) is involved in the oversight, development, implementation, and administration of the Program **(12 CFR 222.90(e)**(1) and (2)).

Comment:

5. Verify that the financial institution trains appropriate staff to effectively implement and

administer the Program (12 CFR 222.90(e)(3)).
Comment:
6. Determine whether the financial institution exercises appropriate and effective oversight of service providers that perform activities related to covered accounts (12 CFR 222.90(e)(4)). See **Appendix** for further guidance on vendor management.
Comment:
7. On the basis of the examination procedures completed, form a conclusion about whether the bank has developed and implemented an effective, comprehensive written Program designed to detect, prevent, and mitigate identity theft.
Comment:
8. Complete the **Summary of Findings.**

SUMMARY OF FINDINGS

ID THEFT RED FLAGS
Describe all strengths evident from the evaluation.
Describe all weaknesses evident from evaluation, including violations of law/regulation/rules; noncompliance with Departmental policies/guidelines; internal policy deficiencies/ noncompliance; internal control weaknesses; MIS problems; and deficiencies in management supervision.
Report Worthy:
Not Report Worthy:
Determine why weaknesses exist and comment on management's response and plan of action. Identify bank personnel making the response.
SUMMARY RISK RATING ASSIGNED: ☐
Definitions:
1-Strong; 2-Satisfactory; 3-Less than satisfactory; 4-Deficient; 5-Critically deficient; NR-Not Rated
(Return to Core Analysis)
Provide copy of this page to EIC/AEIC. Receipt and review of this form by the EIC/AEIC will be evidenced bsy his/her initials in the appropriate column for this procedure on the SCOPE AND REVIEW ACKNOWLEDGEMENT FORM (Planning and Control Worksheet #1).

APPENDIX

IDENTITY THEFT RED FLAGS – 12 CFR 222 SUBPART J (LINK TO REGULATION ON WEB)

The identity theft red flags rule requires a financial institution to periodically determine whether it offers or maintains accounts covered by the regulation. A covered account generally is a consumer account or any other account the institution determines carries a foreseeable risk of identity theft. For covered accounts, an institution must develop and implement a written identity theft prevention program (program) that is designed to detect, prevent, and mitigate identity theft in connection with any new or existing covered account. The program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities. Financial institutions may draw upon their existing programs, such as Bank Secrecy Act/Anti-Money Laundering compliance programs, customer identification programs, or customer information security programs, to help formulate their identity theft prevention program.

Section 615(e) of the Fair Credit Reporting Act requires the federal banking agencies and the National Credit Union Administration (collectively, the Agencies) as well as the Federal Trade Commission to prescribe regulations and guidelines for financial institutions and creditors [1] **regarding identity theft. On November 9, 2007, the Agencies published final rules and guidelines in the Federal Register (72 FR 63718) implementing this section.**

[1] - For purposes of these examination procedures, "financial institutions and creditors" are referred to jointly as "financial institutions.".]

ID Theft Red Flag FAQ

Definitions (12 CFR 222.90(b)). The following regulatory definitions pertain to the regulations regarding identify theft red flags:

1. An "account" is a continuing relationship established by a person with a financial institution to obtain a product or service for personal, family, household, or business purposes. An account includes:
a. An extension of credit, such as the purchase of property or services involving a deferred payment; and

b. A deposit account.

2. The "board of directors" includes, for a branch or agency of a foreign bank, the managing official in charge of the branch or agency and, for any other creditor that does not have a board of directors, a designated employee at the level of senior management.

3. A "covered account" is:
a. An account that a financial institution offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions;

and

b. Any other account offered or maintained by the financial institution for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.

4. A "customer" is a person that has a "covered account" with a financial institution.

5. "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority. "Identifying information" means any name or number that may be used alone or in conjunction with any other information to identify a specific person (16 CFR 603.2).

6. A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

7. A "service provider" is a person that provides a service directly to a financial institution.

Periodic identification of covered accounts (12 CFR 222.90(c)). Each financial institution must periodically determine whether it offers or maintains covered accounts. As part of this determination, the financial institution must conduct a risk assessment to determine whether it offers or maintains covered accounts taking into consideration:

1. The methods it provides to open its accounts;

2. The methods it provides to access its accounts; and

3. Its previous experiences with identity theft.

Establishment of an identity theft prevention program (Program) (12 CFR 222.90(d)). A financial institution must develop and implement a written Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account." The Program must be tailored to the financial institution's size and complexity and the nature and scope of its operations and must contain "reasonable policies and procedures" to:

1. Identify red flags for the covered accounts the financial institution offers or maintains and incorporate those red flags into the Program;

2. Detect red flags that have been incorporated into the Program;

3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

4. Ensure the Program (including the red flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution from identity theft.

Administration of the Program (12 CFR 222.90(e)). A financial institution must provide for the continued administration of the Program by:

1. Obtaining approval of the initial written Program by the board of directors or an appropriate committee of the board;

2. Involving the board of directors, a committee of the board, or an employee at the level of senior management, in the oversight, development, implementation, and administration of the Program;

3. Training staff, as necessary, to implement the Program effectively; and

4. Exercising appropriate and effective oversight of service provider arrangements.

Guidelines (12 CFR 222.90(f)). Each financial institution that is required to implement a program also must consider the guidelines in Appendix J of the regulation and include in its Program those guidelines that are appropriate. The guidelines are intended to assist financial institutions in the formulation and maintenance of a Program that satisfies the regulatory requirements. A financial institution may determine that a particular guideline is not appropriate to incorporate into its Program; however, the financial institution must have policies and procedures that meet the specific requirements of the rules.

Appendix J and Supplement A

A financial institution may incorporate into its Program, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers and to the safety and soundness of the financial institution from identity theft.

Illustrative examples of red flags are located in Supplement A to Appendix J of the regulation. A financial institution is not required to use the examples, nor will it need to justify its failure to include in its Program a specific red flag from the list of examples. However, the financial institution must be able to account for the overall effectiveness of its Program that is appropriate to its size and complexity and the nature and scope of its activities.

(**Return to Core Analysis**)

Vendor Management

1) Is there an effective vendor management program?

If the IT-RMP is performed at the examination, refer to Part V – Vendor Management Program. Confer with the examiner performing Part V to determine if the institution has an adequate vendor management program.

If the IT-RMP is not performed at the examination, refer to Part V of the IT-RMP for questions to consider when assessing the vendor management program.

IT RMP Part V

Also consider the following:

- Each institution should have a vendor management program that includes annual reviews of its significant IT vendors. Some examples of significant IT vendors are the core processor, the electronic banking vendor, and the outsourced network administrator. (Make sure all vendors that have access to covered accounts are included in the vendor review under the VM program.) The vendor management program should be written and approved by the Board of Directors.

  Vendor reviews should include reviews of the vendor's audit reports, SAS70's, financial statements, results of testing, and other similar reports. The reviews should be summarized and reported to the Board at least annually.

- GLBA (FDIC Rules and Regulations, Part 364, Appendix B, Section III (D)) requires that institutions oversee its service provider arrangements and report the oversight to the Board at least annually.

- Refer to FIL-81-2000, Risk Management of Technology Outsourcing for additional guidance.

FIL-81-2000

2) Do contractual agreements with the institution's significant IT vendors address ID Theft Preventions issues? *Future contract renewals and any new contracts should include a provision on ID Theft Prevention issues.*

(Return to Core Analysis)

SUPPLEMENT A TO APPENDIX J

Source:
Federal Reserve System
12 CFR Part 222

Federal Deposit Insurance Corporation
12 CFR Parts 334 and 364

Supplement A to Appendix J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 41.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

- A recent and significant increase in the volume of inquiries;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

- The address does not match any address in the consumer report; or
- The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- The address on an application is the same as the address provided on a fraudulent application; or
- The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

- The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
- The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- Nonpayment when there is no history of late or missed payments;
- A material increase in the use of available credit;
- A material change in purchasing or spending patterns;
- A material change in electronic fund transfer patterns in connection with a deposit account; or
- A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

(**Return to Appendix**)

(**Return to Core Analysis**)